

# Soft-metric based channel decoding for photon counting receivers

Marina Mondin, Fred Daneshgaran, Inam Bari, Maria Teresa Delgado,  
Stefano Olivares, and Matteo G. A. Paris

**Abstract**—We address photon-number-assisted, polarization-based, binary communication systems equipped with photon counting receivers. In these channels information is encoded in the value of polarization phase-shift but the carrier has and additional degree of freedom, i.e. its photon distribution, which may be exploited to implement binary input-multiple output (BIMO) channels also in the presence of a phase-diffusion noise affecting the polarization. Here we analyze the performances of these channels, which approach capacity by means of iteratively decoded error correcting codes. In this paper we use soft-metric-based low density parity check (LDPC) codes for this purpose. In order to take full advantage of all the information available at the output of a photon counting receiver, soft information is generated in the form of log-likelihood ratios, leading to improved frame error rate (FER) and bit error rate (BER) compared to binary symmetric channels (BSC). We evaluate the classical capacity of the considered BIMO channel and show the potential gains that may be provided by photon counting detectors in realistic implementations.

**Index Terms**—Quantum communication, photon detectors

## I. INTRODUCTION

IN binary optical communication, the logical information is encoded onto two different states of the radiation field. After the propagation, the receiver should perform a measurement, aimed at discriminating the two signals. Currently, most of the long-distance amplification-free optical classical communication schemes employ relatively weak laser sources leading to small mean photon count values at the receiver. The same is true for quantum-enhanced secure cryptographic protocols. In fact, laser radiation, which is described by coherent states, preserves its Poissonian photon-number statistics and polarization also in the presence of losses. On the other hand, operating in the regime of low number of detected photons gives rise to the problem of discriminating the signals by quantum-limited measurements [1], [2], [3]. Indeed, the binary discrimination problem for coherent states has been thoroughly investigated, both for its fundamental interest and

for practical purposes [4], [5], [6], [7], [8], [9]. It should be mentioned however that in order to exploit the phase properties of coherent states, one should implement phase sensitive receivers [10], [11] with nearly optimal performances also in the presence of dissipation and noise [7], [12]. This is a challenging task, since it is generally difficult, and sometimes impossible, to have a suitable and reliable phase reference in order to implement this kind of receiver [13].

The simplest choice for a detection scheme involving radiation is given by detectors which simply reveal the presence or the absence of radiation (on/off detectors) with acceptable dead-time values and dark count rates. A natural evolution of such schemes would be to employ photon counting receivers. Indeed, development of photon counters has been extensively pursued in the last decades, as well as of methods to extract the photon distribution by other schemes [14], [15], [16], [17], [18]. Given that one could use photon counting detectors for weak-energy optical communications, a question arises on whether and how such detectors may be employed to improve the system performance. A possible way to answer this question is to determine the capacity of the corresponding optical channels, and the achievable residual Bit Error Rate (BER) and Frame Error Rate (FER) of practical communication schemes over these channels. A photon counting detector is clearly able to extract more information than a simple on/off detector. The practical consequence is that a photon counting detector allows one to generate a meaningful log-likelihood (i.e. a soft-metric), as opposed to a hard-metric allowed by a hard- (or on/off) detector. Furthermore, soft-metrics lead to improved performances when exploited by powerful iteratively decoded forward error correcting codes.

Recently, a simple polarization-based communication scheme involving weak coherent optical signals and low-complexity photon counting receivers has been presented [1], and its performances have been analyzed based on an equivalent Binary Symmetric Channel (BSC) model of the overall scheme. In this paper, we extend the scheme of [1] and model the effect of the photon distribution of the coherent signals as a time varying Binary Input-Multiple Output (BIMO) channel. In particular, we employ soft-metric based Low Density Parity Check (LDPC) codes for transmission over the BIMO channel to approach capacity using iteratively decoded error correcting codes and investigate the potential improvements that may be obtained in terms of classical capacity and residual BER using photon counting receivers [27]. It is worth noting that recently photon-counting detectors have been proposed to enhance the discrimination of weak optical signal in the case of  $M$ -

M. Mondin is with the Dipartimento di Elettronica e Telecomunicazioni, Politecnico di Torino, 10129 Torino, Italy, e-mail: marina.mondin@polito.it

F. Daneshgaran is with the Electrical and Computer Eng. Dept., California State Univ., Los Angeles, CA, USA, e-mail: fdanesh@calstatela.edu

I. Bari is with the National University of Computer and Emerging Sciences (FAST-NU), Peshawar, Pakistan e-mail: inam.bari@nu.edu.pk

M. T. Delgado is with the Dipartimento di Elettronica e Telecomunicazioni, Politecnico di Torino, 10129 Torino, Italy, e-mail: maria.delgadoalizo@polito.it

S. Olivares is with the Dipartimento di Fisica, Università degli Studi di Milano, I-20133 Milano, Italy, e-mail: stefano.olivares@fisica.unimi.it

M. G. A. Paris is with the Dipartimento di Fisica, Università degli Studi di Milano, I-20133 Milano, Italy, e-mail: matteo.paris@fisica.unimi.it

any coherent state discrimination [28], [29]: in these cases, however, a suitable feedback scheme or the use of squeezing are required.

The receiver introduced in [1] is based on an optical setup for one-parameter qubit gate optimal estimation [2], [21], [19]. In this scheme, the qubit is encoded in the polarization degree of freedom of a light beam, whose intensity (photon) degree of freedom has been prepared in a coherent state, and the one-parameter gate corresponds to a polarization transformation. In the ideal case, orthogonal polarization states can be perfectly discriminated. However, in a realistic scenario and especially in free-space communication, non-dissipative (diffusive) noise affecting light polarization disturbs the orthogonality of the states at the receiver, thus requiring suitable detection and strategy for discrimination. It is worth noting that coherent states preserve their fundamental properties when propagating in purely lossy channels, suffering only attenuation, thus only the noise affecting the polarization is detrimental. Remarkably, since our receiver is phase-insensitive, the scheme works as well as when phase-diffusion noise is affecting the channel. This also holds in the case of phase-randomized coherent states [22] which can be easily generated, characterized and manipulated [23] and are useful for enhancing security in decoy state quantum key distribution [24], [25].

The paper is organized as follows; the physical system is described in Section II, where the corresponding channel model and log-likelihood metric are also defined. The associated channel capacity is evaluated in Section IV, while the achievable residual frame and bit error rate obtained with LDPC coding is presented in Section V. Section VI concludes the paper with some final remarks.

## II. THE PHYSICAL CHANNEL

The channel we are going to investigate corresponds to the optical setup schematically depicted in Fig. 1. The information bit is encoded onto the polarization degree of freedom of a light beam prepared in a coherent state  $|\alpha\rangle$ , initially linearly polarized at  $45^\circ$  with respect to the  $x$ -axis, i.e.:

$$|\alpha\rangle \otimes |+\rangle = |\alpha\rangle \otimes \left( \frac{|H\rangle + |V\rangle}{\sqrt{2}} \right),$$

where  $|H\rangle$  and  $|V\rangle$  denote horizontal and vertical polarization states with respect to the  $x$ -axis. The encoding rule for the bit  $k = 0, 1$  is applied to the qubit by means of the polarization rotation  $U(\phi_k) = e^{-i\frac{1}{2}\phi_k\sigma_3}$ ,  $\sigma_3$  being the Pauli matrix. Due to the analogy with the phase-shift encoding, from now on we will refer to  $U(\phi_k)$  as “phase shift”. In order to follow the scheme proposed in Refs. [1] and in view of a possible experimental verification reported in [21], [19], we assume that the encoding rule for the bit given in Table I.

$k$	$\longrightarrow$	$\phi_k$
0	$\longrightarrow$	$\pi/4$
1	$\longrightarrow$	$3\pi/4$

Table I

ENCODING RULE FOR THE POLARIZATION PHASE-SHIFT.



Figure 1. Schematic diagram of the optical setup implementing photon-number-assisted, polarization-based, binary communication channels equipped with photon counting receivers.

The polarization rotation (phase shift) may be easily implemented by means of a KDP crystal driven by a high voltage generator, and corresponds to a change of the polarization from linear to elliptical. At the detection stage information is retrieved by intensity measurement, in a scheme involving a Half-Wave Plate (HWP), a Polarizing Beam Splitter (PBS) and two photon counters. This scheme has been experimentally tested to achieve one-parameter qubit gate optimal estimation [21], [19]. Furthermore, several examples of detectors now used by the quantum optics community, can be used as photon counters [15], [16], [17], [21], [22], [23]. The outcomes of the measurement are thus pairs of integer numbers  $(n_0, n_1)$ , where  $n_k$  is the number of detected photons in the reflected ( $k = 0$ ) and transmitted ( $k = 1$ ) beam, respectively. Notice that the total number of detected photons  $n = n_0 + n_1$  is varying shot by shot. We assume that no photon is lost at the beam splitter. The number of photons in the coherent carrier is a Poisson distributed random variable with mean value  $N_c = |\alpha|^2$ . Also the two beams after the PBS are coherent states and the joint probability of obtaining the outcome  $(n_0, n_1)$  is the product of two factorized Poisson distributions. The mean values depend on the polarization phase-shift, i.e. on the bit value. Upon denoting by  $N_k(\phi)$  the mean photon number in the reflected or transmitted beam when the imposed phase-shift is  $\phi$ , we have:

$$N_0(\phi) = \frac{1}{2}N_c(1 + \cos \phi), \quad N_1(\phi) = \frac{1}{2}N_c(1 - \cos \phi).$$

The probability of the event  $(n_0, n_1)$  is thus given by:

$$\begin{aligned} p(n_0, n_1 | \phi) &= e^{-N_0(\phi) - N_1(\phi)} \frac{N_0(\phi)^{n_0}}{n_0!} \frac{N_1(\phi)^{n_1}}{n_1!} \\ &= e^{-N_c} \frac{N_0(\phi)^{n_0}}{n_0!} \frac{N_1(\phi)^{n_1}}{n_1!}. \end{aligned} \quad (1)$$

The overall scheme is suitable for working with weak optical signals, where the value of  $N_c$  is typically small. The relevant observation to be made here is that the information is retrieved by photon counting, and therefore the discrete bit value  $k$ , encoded in the polarization qubit, is mapped at the detection stage onto pairs of integer numbers. The considered scheme can be modeled as shown in Fig. 2, i.e. with an equivalent binary-input/multiple-output channel that receives the binary random variable  $k$  as input, and generates the two random variables  $n_0, n_1$  as outputs. In particular, for a given number  $n$  of detected photons, there are  $n + 1$  pairs  $n_0, n_1$  such that  $n_0 + n_1 = n$ . The availability of multiple outputs, whose

likelihood can be exploited for soft-information processing, is a crucial characteristic of the described scheme.

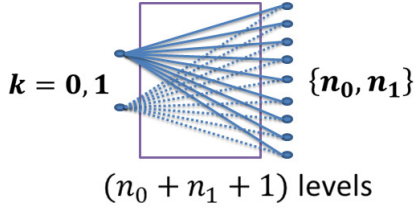


Figure 2. BIMO channel model of the considered system.

If propagation of the light beam occurs in an environment, which perturbs the polarization but preserves the energy, then the state impinging onto the PBS has no longer a well-defined polarization (phase): If the initial state is  $|\phi_k\rangle \otimes |\alpha\rangle$ , where  $|\phi_k\rangle = U(\phi_k)|+\rangle$  refers to the polarization qubit, the phase-diffusion noise affects the polarization according to the map [21]:

$$|\phi_k\rangle \rightarrow \varrho_k = \int_{\mathbb{R}} d\varphi g(\varphi, \Delta) U(\varphi) |\phi_k\rangle \langle \phi_k| U^\dagger(\varphi), \quad (2)$$

where  $\varrho_k$  represents the density matrix of the degraded polarization qubit and  $g(\varphi, \Delta)$  is a normal distribution of the variable  $\varphi$  with zero mean and standard deviation  $\Delta$ . From the physical point of view, Eq. (2) follows from a Master equation approach [30] which represents a dynamics in which the quantum state of light undergoes an energy conserving scattering affecting the polarization. Overall, this corresponds to applying a random polarization rotation (or phase shift) of the input polarization distributed according to  $g(\varphi, \Delta)$ . The probabilities of the outcomes are still given by Eq. (1), however with the mean photon numbers modified to:

$$N_0(\phi, \Delta) \equiv N_0(\phi) = \frac{1}{2} N_c (1 + e^{-\Delta^2} \cos \phi), \quad (3)$$

$$N_1(\phi, \Delta) \equiv N_1(\phi) = \frac{1}{2} N_c (1 - e^{-\Delta^2} \cos \phi). \quad (4)$$

### III. EVALUATION OF THE LOG-LIKELIHOOD RATIOS

Soft-decoding algorithms are typically based on the use of Log-Likelihood-Ratios (LLR). In our particular case, the LLR values associated to the channel model of Fig. 2 can be evaluated as:

$$\text{LLR}(n_0, n_1) = \log_2 \left[ \frac{p(\phi_1 | n_0, n_1)}{p(\phi_0 | n_0, n_1)} \right] \quad (5)$$

where,

$$p(\phi_k | \{n_0, n_1\}) \quad k = 0, 1 \quad (6)$$

is the probability that the transmitted bit was “ $k$ ” given the outcomes  $(n_0, n_1)$ . Using Bayes theorem, Eq. (5) may be rewritten as:

$$\text{LLR}(n_0, n_1) = \log_2 \left[ \frac{p(n_0, n_1 | \phi_1)}{p(n_0, n_1 | \phi_0)} \right]. \quad (7)$$

Finally, using Eq. (1) we arrive at:

$$\text{LLR}(n_0, n_1) = (n_0 - n_1) \log_2 \left( \frac{q}{1 - q} \right) \quad (8)$$

where,

$$q = \frac{1}{2} \left[ 1 - e^{-\Delta^2} \cos \left( \frac{\pi}{4} \right) \right], \quad (9)$$

for the chosen encoding. The system described up to this point represents, for a given  $n$ , a BIMO Discrete Memoryless Channel (DMC) [20] with binary input  $k$  and  $n + 1 = n_0 + n_1 + 1$  outputs  $(n_0, n_1)$ , where  $n$  is a Poisson distributed random variable. In the next Section we will evaluate the capacity of this channel.

### IV. EVALUATION OF CAPACITY

A sufficient statistic for detection with photon counting detectors is the difference photocurrent at the output, i.e.  $D = n_1 - n_0$ . Since the two random variables  $n_0$  and  $n_1$  are Poisson distributed, the outcome  $d$  of  $D$  is Skellam distributed, namely:

$$p_D(d|\phi) = e^{-N_c} \left[ \frac{N_1(\phi)}{N_0(\phi)} \right]^{d/2} I_{|d|} \left( 2\sqrt{N_1(\phi)N_0(\phi)} \right), \quad (10)$$

where  $I_m(z)$  is the modified Bessel function of the first kind, such that:

$$p_D(d|\phi_k) = e^{-N_c} \left( \frac{q}{1 - q} \right)^{(-1)^k d/2} I_{|d|} \left( 2N_c \sqrt{q(1 - q)} \right). \quad (11)$$

Upon denoting by  $\Phi$  the input binary variable, the relevant figure of merit to evaluate the channel capacity is the mutual information:

$$I(\Phi, D) = H(\Phi) - H(\Phi|D),$$

where,

$$H(\Phi) = -z_0 \log_2 z_0 - z_1 \log_2 z_1,$$

is the Shannon entropy of the input alphabet,  $z_0$  ( $z_1 = 1 - z_0$ ) being the a-priori probability of sending the bit  $k = 0$  ( $k = 1$ ) and  $H(\Phi|D)$  is the conditional entropy:

$$H(\Phi|D) = - \sum_{k,d} p_D(d) p(\phi_k | d) \log_2 p(\phi_k | d)$$

and,

$$p_D(d) = z_0 p_D(d|\phi_0) + (1 - z_0) p_D(d|\phi_1) \quad (12)$$

is the overall probability of the outcome  $d$ , irrespective of the input bit.

Our BIMO DMC is neither symmetric nor weakly symmetric. Recall that a DMC is said to be symmetric if the rows (and the columns) of the channel transition probability matrix are permutations of each other. If, on the other hand, the rows are permutations of each other and the column sums are equal but the columns are not permutations of each other, the DMC is said to be weakly symmetric. It can be shown that for symmetric or weakly symmetric channels uniform probability on input maximizes the mutual information thus yielding capacity. However, it can be easily shown that the input probability distribution maximizing the mutual information in

the BIMO case above is the uniform one, i.e.  $z_0 = z_1 = 1/2$ . The channel capacity is thus given by:

$$\begin{aligned} \mathcal{C} &= \max_{z_0} I(\Phi|D) \\ &= 1 + \frac{1}{2} \sum_{k,d} [p_D(d|\phi_0) + p_D(d|\phi_1)] p(\phi_k|d) \log_2 p(\phi_k|d). \end{aligned} \quad (13)$$

Our goal is now to compare the capacity of the present photon counting receiver channel to that of the equivalent binary symmetric channel resulting from the detection of optical signals by on/off receiver, which just discriminates the presence or the absence of radiation (i.e., performs hard decoding). The transition probability of the equivalent BSC associated with the considered photon counting receiver (i.e. the raw BER, denoted in the following as QBER) can be obtained as:

$$\text{QBER} = \sum_{m=1}^{\infty} p_D(m|\phi_0) + \frac{1}{2} p_D(0|\phi_0), \quad (14)$$

$$= \sum_{m=1}^{\infty} p_D(-m|\phi_1) + \frac{1}{2} p_D(0|\phi_1). \quad (15)$$

Essentially, assuming  $\phi_0$  is true, a detection error occurs for a hard decision detector if  $D = n_1 - n_0 > 0$ . In case  $D = 0$ , the detector can toss a fair coin and assign a decoded bit arbitrarily, in which case the probability of error is  $\frac{1}{2} p_D(0|\phi_1)$ .

In our case, in the limit  $N_c \gg 1$ , we can write:

$$\frac{N_1(\phi_k)}{N_2(\phi_k)} = \frac{p(1|\phi_k)}{p(0|\phi_k)}$$

and,

$$N_1(\phi_k) N_2(\phi_k) = N_c^2 p(1|\phi_k) p(0|\phi_k).$$

When “0 is transmitted and it is mapped to  $\phi_0$ ”, we get from Eqs. (3) and (4):

$$p_D(m|\phi_0) = \frac{e^{-N_c}}{\sqrt{\alpha_\Delta^m}} B_m(N_c, \Delta);$$

analogously when “1 is transmitted and it is mapped to  $\phi_1$ ”:

$$p_D(m|\phi_1) = e^{-N_c} \sqrt{\alpha_\Delta^m} B_m(N_c, \Delta),$$

where,

$$\alpha_\Delta = \frac{\sqrt{2} + e^{-\Delta^2}}{\sqrt{2} - e^{-\Delta^2}},$$

and,

$$B_m(N_c, \Delta) = I_{|m|} \left( N_c \sqrt{1 - \frac{1}{2} e^{-2\Delta^2}} \right).$$

After some manipulation we have:

$$\begin{aligned} p_{0,m} &\equiv p(\phi_0|D = m) = \frac{z_0}{z_0(1 - \alpha_\Delta^m) + \alpha_\Delta^m}, \\ p_{1,m} &\equiv p(\phi_1|D = m) = \frac{1 - z_0}{z_0(1 - \alpha_\Delta^m) + \alpha_\Delta^m}. \end{aligned}$$

The final expression of the conditional entropy as a function of the two parameters  $N_c$  and  $\Delta$  is:

$$\begin{aligned} H(\Phi|D) &= -e^{-N_c} \sum_m \frac{z_0 B_m(N_c, \Delta)}{\sqrt{\alpha_\Delta^m}} \log_2(p_{0,m}) \\ &\quad - e^{-N_c} \sum_m (1 - z_0) B_m(N_c, \Delta) \sqrt{\alpha_\Delta^m} \log_2(p_{1,m}). \end{aligned}$$

Note that capacity is achieved with  $z_0 = \frac{1}{2}$ . The results are shown in Fig. 3 and 4. The capacity of the BIMO DMC compared to that of the equivalent BSC obtained in case of on/off detection is shown in Fig. 3 as a function of the mean photon number  $N_c$  and for  $\Delta = 0, 0.5$ , while in Fig. 4 the BIMO DMC is compared to the equivalent BSC for  $N_c = 1, 3, 7, 12$  as a function of the phase diffusion parameter  $\Delta$ . It is possible to observe that a higher capacity can be obtained by the BIMO DMC with respect to the equivalent BSC, that may possibly lead to improved BER improvement when an error correction code is applied to the two channels. This aspect is indeed investigated in the next section. The capacity improvement offered by the photon counting detector decreases as  $N_c$  increases, in particular for low values of  $\Delta$ , as it can be observed by both Fig. 3 and Fig. 4.

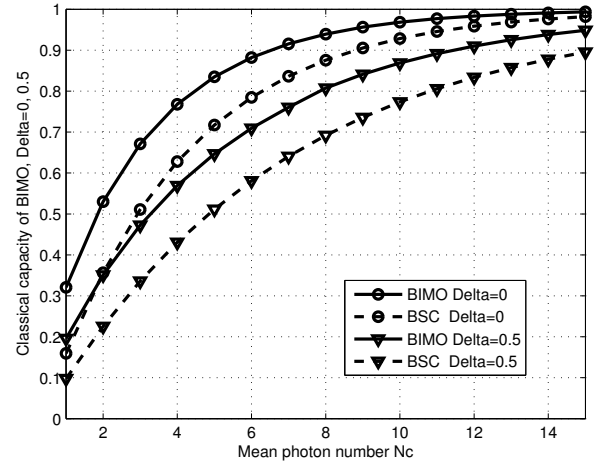


Figure 3. Classical capacity of the equivalent BSC with cross-over probability QBER (dashed curves) compared to that of the BIMO DMC (solid curves) for  $\Delta = 0$  (circle) and  $\Delta = 0.5$  (triangle) as a function of mean photon number  $N_c$ .

## V. BER PERFORMANCE IN PRESENCE OF FEC

This section investigates the performance obtainable with Forward Error Correction (FEC) codes applied to the scheme of Figs. 1 and 2. The  $m$ -bits codeword of a systematic FEC code with code rate  $R_c$  is generated concatenating  $L$  information bits and  $r$  redundancy bits so that  $m = L + r$  and  $R_c = L/(L + r)$ .

A systematic low density parity check code has been selected as test FEC code, due to its capacity achieving performance (albeit at very large block lengths) and low complexity iterative decoding structure, and a simulation analysis has been performed to assess the potential performance improvements

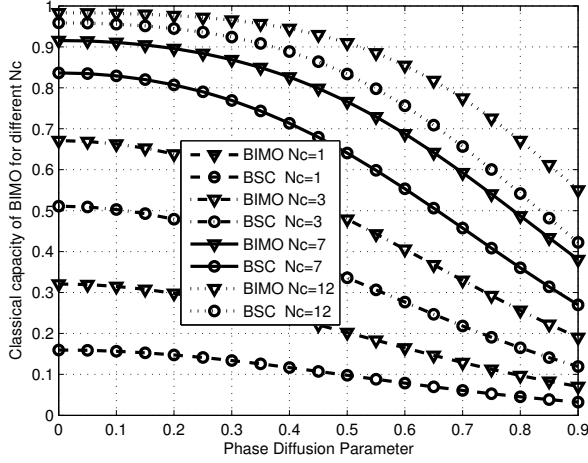


Figure 4. Classical capacity of equivalent BSC with cross-over probability QBER (circle) and of BIMO DMC (triangle) for  $N_c = 1, 3, 7, 12$  as a function of the phase diffusion parameter  $\Delta$ .

obtainable using the soft-metric of Eq. (8). Three different quantum channel models have been considered, all with the same equivalent uncoded raw BER value, that will be denoted as QBER. The simulation results are shown in Fig. 5, where each pair of BER-FER curves depicts the residual bit error rate and frame error rate after channel decoding. The following parameters have been considered:

- $R_c = 0.5$ ,  $L = 500$ ,  $r = 500$ ,
- $R_c = 0.61$ ,  $L = 252$ ,  $r = 156$ ,
- $R_c = 0.75$ ,  $L = 750$ ,  $r = 250$ .

The black curves in Fig. 5 labeled "Q-BSC" are associated with an equivalent BSC with binary input  $X = k$ , binary output  $Y$  and transition probability QBER derived from Eq. (15) (i.e. a receiver that does not use the additional information derived from the knowledge of  $n_0$  and  $n_1$  and simply performs on/off detection) with LLR values [26]:

$$\begin{aligned} \text{LLR}(Y) &= \log_2 \left[ \frac{P(Y=1|X)}{P(Y=0|X)} \right] \\ &= \begin{cases} \log_2 \left( \frac{1-\text{QBER}}{\text{QBER}} \right), & \text{if } X = 1; \\ \log_2 \left( \frac{\text{QBER}}{1-\text{QBER}} \right), & \text{if } X = 0. \end{cases} \end{aligned}$$

The blue curves labeled as "Q-AWGN" represent the performance obtainable over a fictitious Additive White Gaussian Noise (AWGN) channel model with a Signal to Noise Ratio (SNR) selected in order to achieve an uncoded bit error probability QBER with a binary antipodal scheme. The curves labeled as "Q-BIMO" represent the main result and are obtained transmitting through the BIMO DMC quantum channel model shown in Fig. 2 with equivalent uncoded bit error probability QBER and using as input soft-metrics for the LDPC decoder, the LLR values generated via photon counting according to Eq. (8).

As it is apparent from the results for the photon counting receiver, the BER and FER performance largely improve when the BIMO DMC and the LLR metrics from Eq. (8) are

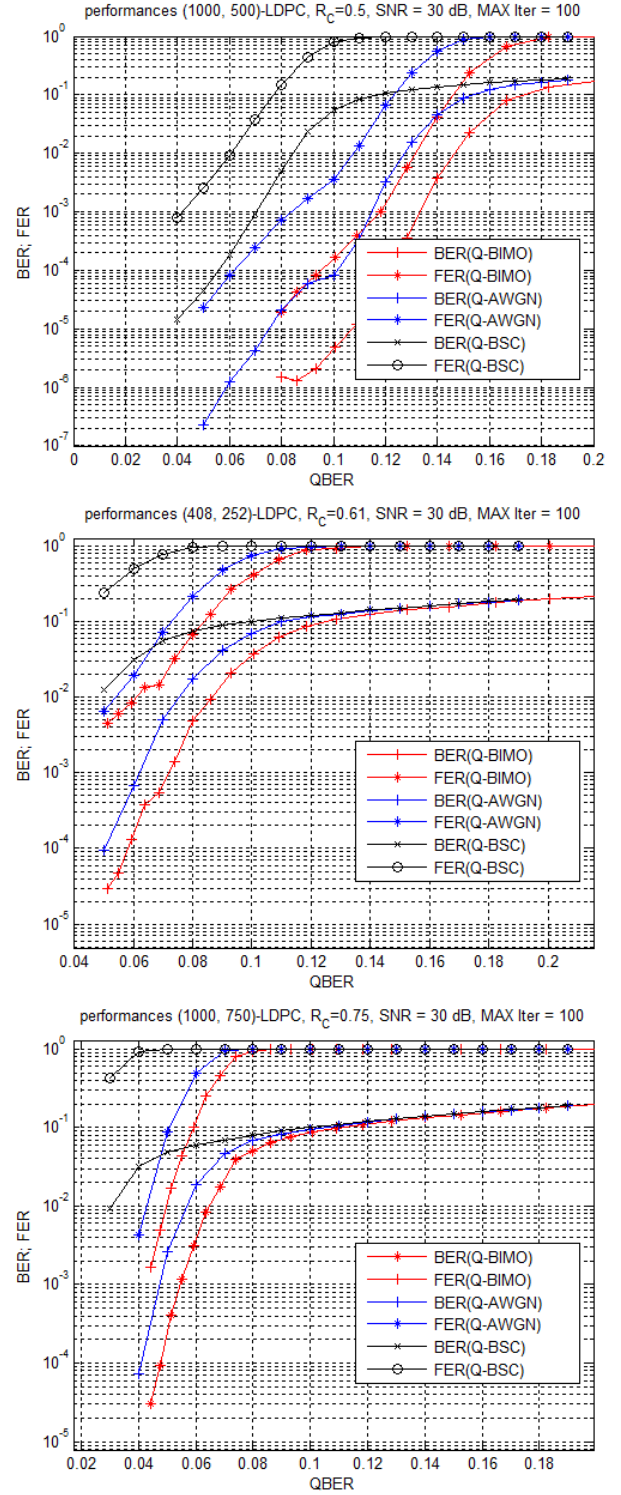


Figure 5. Simulated BER and FER values for a LDPC code with  $L = 500$ ,  $r = 500$  and  $R_c = 0.5$  (top plot),  $L = 252$ ,  $r = 156$  and  $R_c = 0.61$  (center plot) and  $L = 750$ ,  $r = 250$  and  $R_c = 0.75$  (bottom plot), obtained with different models of the quantum channel: BSC (Q-BSC curves, black), AWGN (Q-AWGN curves, blue) and BIMO DMC (Q-BIMO curves, red).

employed instead of the simpler BSC metrics. As an example, in the upper plot in Fig. 5 for  $\text{QBER} = 0.1$  the BIMO DMC with soft-metric processing offers almost three orders of magnitude improvement in BER with respect to the BSC



model and the associated hard-metric processing. We must note that the curves labeled as “Q-AWGN” must only be used as reference, since with the small number of photons we considered in our simulations the AWGN channel model would not be appropriate.

A comparison among the residual FER and BER values obtainable with the considered channel models for LDPC codes with code rates 0.61 (center plot) and 0.75 (bottom plot) is shown in Fig. 5. Also in these cases, both FER and BER values improve up to several orders of magnitude when using a photon counting receiver and the associated LLR values. Furthermore, we can observe that as the code rate increases, the “Q-BIMO” performances obtained with BIMO LLR metrics get closer to the “Q-AWGN” performances obtained with classic AWGN LLR metrics (although, as mentioned before, the AWGN model is not applicable in case of low number of received photons).

Fig. 6 compares the BER values obtained with the BSC and the BIMO channel models for different code rates, showing that, as expected, for higher rates, a lower QBER value is required before significant coding gains can be observed.

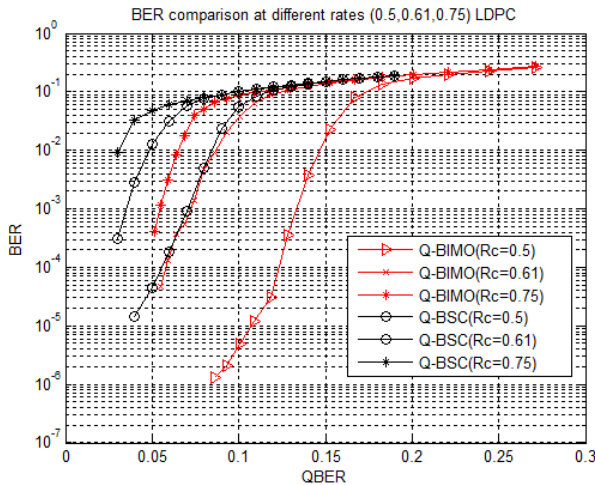


Figure 6. Simulated residual BER obtained with BSC (Q-BSC curves, black) and BIMO DMC (Q-BIMO curves, red) models of the quantum channel and LDPC codes with different code rates ( $R_c = 0.5, 0.61$  and  $0.75$ ).

From Fig. 7, we can observe that for high values of  $N_c$  (i.e. at low values of QBER) the BIMO DMC model can be approximated with an AWGN model, while the AWGN model approximation may be unreliable at high QBER (low  $N_c$ ) values, in particular at lower code rate values. Finally, Fig. 8 shows the residual BER obtained on the BIMO channel by LDPC codes with code rate  $R_c = 0.5, 0.61, 0.75$  for different values of  $N_c$ .

## VI. CONCLUSIONS

In this paper a photon-number-assisted, polarization-based binary transmission scheme equipped with a low-complexity photon counting receiver has been considered, analyzing both its capacity and its BER performance in presence of capacity achieving low density parity check codes. Different channel models applicable to the considered transmission

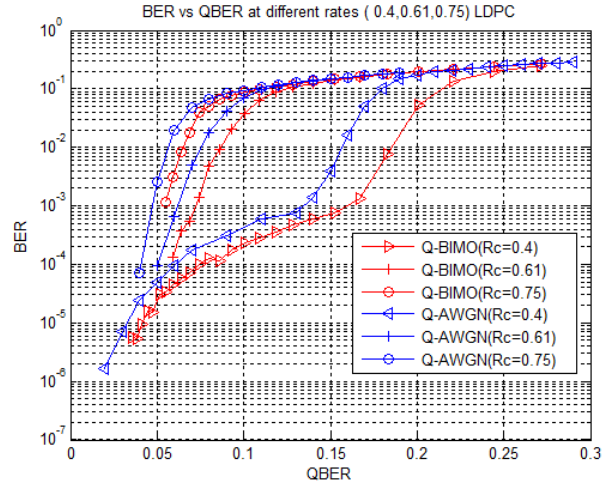


Figure 7. Simulated residual BER obtained with AWGN (Q-AWGN curves, blue) and BIMO DMC (Q-BIMO curves, black) models of the quantum channel and LDPC codes with different code rates ( $R_c = 0.4, 0.61$  and  $0.75$ ).

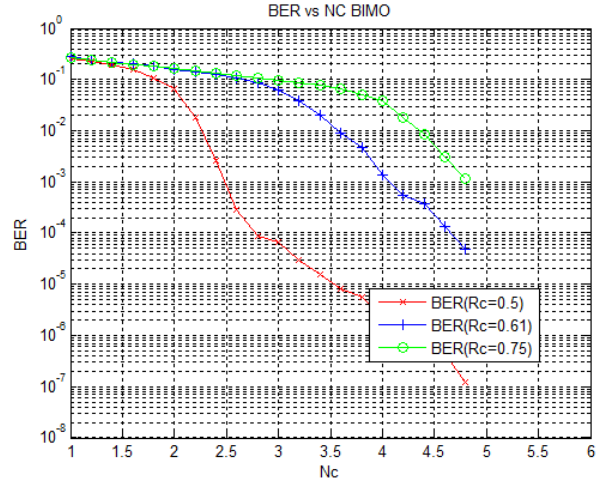


Figure 8. Simulated residual BER for LDPC codes with  $R_c = 0.5, 0.61, 0.75$  over BIMO DMC as a function of the mean photon number  $N_c$ .

scheme have been compared, proposing a time varying binary-input/multiple-output model and evaluating its LLR metrics and channel capacity. It has been shown how the BIMO channel model outperforms the corresponding BSC model, by taking full advantage of the additional information offered by the photon counting detector. It was also shown that, as expected, the advantage offered by the photon counting detector decreases as the mean photon number  $N_c$  increases, and that the BIMO model can be approximated by an AWGN model at low values of QBER, i.e. for high values of  $N_c$ .

## ACKNOWLEDGMENT

This work was supported by MIUR (grant FIRB “LiCHIS” - RBFR10YQ3H) and NATO (SfP project 984397 “Secure Quantum Communications”).

## REFERENCES

- [1] S. Olivares, M. G. A. Paris, M. Delgado, and M. Mondin, "Toward a soft output quantum channel via Bayesian estimation", in 3rd International Symposium on Applied Sciences in Biomedical and Communication Technologies (ISABEL), pp.1-2, Nov. 7-10, 2010.
- [2] B. Teklu, S. Olivares, and M. G. A. Paris, "Bayesian estimation of one-parameter qubit gates", *J. Phys. B: At. Mol. Opt. Phys.*, vol. 42, art. no. 0335502, 2009.
- [3] N. Tomassoni, M. G. A. Paris, "Quantum binary channels with mixed states" *Phys. Lett. A*, vol. 373, pp. 61-64, 2008.
- [4] R. S. Kennedy, Research Laboratory of Electronics, MIT, Quarterly Progress Report No. 108, 1973, p. 219 (unpublished).
- [5] S. J. Dolinar, Jr., "An Optimum Receiver for the Binary Coherent State Quantum Channel", MIT Research Laboratory of Electronics Quarterly Progress Report 111, Cambridge, Massachusetts, pp. 115-120, October 15, 1973.
- [6] M. Sasaki, and O. Hirota, "Optimum decision scheme with a unitary control process for binary quantum-state signals", *Phys. Rev. A*, vol. 54, pp.2728- 2736, 1996.
- [7] S. Olivares, and M. G. A. Paris, "Binary optical communication in single-mode and entangled quantum noisy channels", *J. Opt. B: Quantum and Semiclass. Opt.*, vol. 6, pp. 69-80, 2004.
- [8] J. M. Geremia, "Distinguishing between optical coherent states with imperfect detection", *Phys. Rev. A*, vol. 70, art. no. 062303, 2004.
- [9] M. Takeoka, M. Sasaki, P. van Loock, and N. Lutkenhaus, "Implementation of projective measurements with linear optics and continuous photon counting", *Phys. Rev. A*, vol. 71, art. no. 022318, 2005.
- [10] C.-W. Lau, V. A. Vilmotter, S. Dolinar, J. M. Geremia, and H. Mabuchi, "Binary Quantum Receiver Concept Demonstration", IPN Progress Report 42-165, 1, 2006.
- [11] R. L. Cook, P. J. Martin, and J. M. Geremia, "Optical coherent state discrimination using a closed-loop measurement", *Nature*, vol. 466, pp. 774-777, 2007.
- [12] C. Wittmann, U. L. Andersen, M. Takeoka, D. Sych, and G. Leuchs, "Discrimination of binary coherent states using a homodyne detector and a photon number resolving detector", *Phys. Rev. A*, vol. 81, art. no. 062338, 2010.
- [13] M. Bina, A. Allevi, M. Bondani, and S. Olivares, "Real-time phase-reference monitoring of a quasi-optimal coherent-state receiver" Preprint arXiv:1408.0228 [quant-ph] (2014).
- [14] A. R. Rossi, S. Olivares and M. G. A. Paris, "Photon statistics without counting photons", *Phys. Rev. A*, vol. 70, art. no. 055801, 2004; M. Bondani, G. Zambra, A. Andreoni, M. Gramegna, M. Genovese, G. Brida A. Rossi and M. G. A. Paris, "Experimental reconstruction of photon statistics without photon counting", *Phys. Rev. Lett.* vol. 95, art. no. 063602, 2005.
- [15] M. Bondani, A. Allevi, A. Agliati, and A. Andreoni, *J. Mod. Opt.*, "Self-consistent characterization of light statistics", vol. 56, pp. 226-231, 2009.
- [16] A. Allevi, A. Andreoni, M. Bondani, G. Brida, M. Genovese, M. Gramegna, S. Olivares, M. G. A. Paris, P. Traina, and G. Zambra, "State reconstruction by on/off measurements", *Phys. Rev A* vol. 80, art. no. 022114, 2009.
- [17] A. Allevi, A. Andreoni, M. Bondani, M. G. Genoni, and S. Olivares, "Reliable source of conditional states from single-mode pulsed thermal fields by multiple-photon subtraction", *Phys. Rev. A*, vol. 82, art. no. 013816, 2010.
- [18] D. A. Kalashnikov, S. H. Tan, M. V. Chekhova, and L. A. Krivitsky "Accessing photon bunching with a photon number resolving multi-pixel detector", *Optics Express*, vol. 19, pp. 9352-9363, 2011.
- [19] M. G. Genoni, S. Olivares, and M. G. A. Paris, "Optical phase estimation in the presence of large phase diffusion", *Phys. Rev. Lett.*, vol. 106, art. no. 153603, 2011.
- [20] T. M. Cover and J. A. Thomas, *Elements of Information Theory*, John Wiley & Sons, Inc. 1991.
- [21] D. Brivio, S. Cialdi, S. Vezzoli, B. Teklu, M. G. Genoni, S. Olivares, and M. G. A. Paris, "Experimental estimation of one-parameter qubit gates in the presence of phase diffusion", *Phys. Rev. A*, vol. 81, art. no. 012305, 2010.
- [22] G. Zambra, A. Allevi, M. Bondani, A. Andreoni, and M. G. A. Paris, "Nontrivial photon statistics with low resolution-threshold photon counters", *Int. J. Quantum Inf.*, vol. 5, pp. 305-309, 2007.
- [23] A. Allevi, S. Olivares, and M. Bondani, "Manipulating the non-Gaussianity of phase-randomized coherent states", *Opt. Express*, vol. 20, pp. 24850-24855, 2012.
- [24] H.-K. Lo, and J. Preskill, CALT-68-2556, e-print arXiv:quant-ph/0504209v, 2005.
- [25] M. Curty, X. Ma, B. Qi, and T. Moroder, "Passive decoy-state quantum key distribution with practical light sources", *Phys. Rev. A*, vol. 81, art. no. 022310, 2010.
- [26] M. Mondin, M. Delgado, F. Mesiti, F. Daneshgaran, "Soft-processing for Information Reconciliation in QKD Applications", *Int. J. Quant. Inf.*, vol. 9, pp. 155-164, 2011.
- [27] M. Mondin, F. Daneshgaran, I. Bari, M. T. Delgado, "Capacity approaching codes for photon counting receivers", Proc. of SPIE Optics+Photonics 2012 (Quantum Communications and Quantum Imaging X), San Diego, California, USA, August 11-16, 2012.
- [28] K. Li, Y. Zuo, and B. Zhu, *IEEE Photon. Technol. Lett.* vol. 25, 2182-2184, 2013.
- [29] S. Izumi, M. Takeoka, K. Ema, and M. Sasaki, *Phys. Rev. A* vol. 87, art. no. 042328, 2013.
- [30] C. W. Gardiner and P. Zoller, *Quantum Noise*, Springer, 2004.

**Marina Mondin** is Associate Professor at Dipartimento di Elettronica, Politecnico di Torino. Her current interests are in the area of signal processing for communications, modulation and coding, simulation of communication systems, and quantum communication. She holds two patents. She has been Associate Editor for IEEE Transactions on Circuits and Systems-I from 2010 to 2013 and has been in the 2012 TCAS committee for the selection of the Darlington and Guillemin-Cauer Best Paper Awards. She is currently coordinating the NATO SfP project "Secure Communication Using Quantum Information Systems". She is author of more than 150 publications.

**Fred Daneshgaran** received the Ph.D. degree in electrical engineering from University of California, Los Angeles (UCLA), and since 1997 has been a full Professor with the ECE Department at California State University, Los Angeles (CSLA). From 2006 he serves as the chairman of the ECE department. Dr. Daneshgaran is the founder of Euroconcepts, S.r.l, a R&D company specializing in the design of advanced communication links and software radio that operated from 2000 to 2010. From 1999 to 2001 he was the Chief Scientist and member of the management team, for TechnoConcepts, Inc. where he directed the development of a prototype software defined radio system, managed the hardware and software teams and orchestrated the entire development process. He is the director of the fiber and non-linear optics research laboratory at CSLA, and served as the Associate Editor of the IEEE Trans. On Wireless Comm. in the areas of modulation and coding, multirate and multicarrier communications, broadband wireless communications, and software radio, from 2003 to 2009. He has served as a member of the Technical Program Committee (TPC) on numerous conferences. Most recent contributions include IEEE WCNC 2014, CONWIRE 2012, ISCC 2011 to 2014, and PIMRC 2011.

**Inam Bari** Inam Bari obtained his BS in Telecommunication Engineering from the National University of Computer and Emerging Science (NUCES-FAST), Pakistan in 2007, and was awarded bronze medal. In 2008, he was awarded a full 5 years MS leading to PhD scholarship by the Higher Education Commission of Pakistan. He obtained his MS and PhD degrees from Politecnico di Torino, Italy, and is currently Assistant Professor at NUCES-FAST, Peshawar, Pakistan.

**Maria Teresa Delgado** received her BS Degree in Electrical Engineering at the Universidad Central de Venezuela in Caracas, Venezuela in 2006, and her MS and Ph.D. degrees in Telecommunication Engineering from Politecnico di Torino, Italy, in 2008 and 2012. Her interests are in the area of signal processing for telecommunications, coding, simulation of communication systems, quantum cryptography and physical layer security for wireless and quantum communication systems. She is currently researcher at Istituto Superiore Mario Boella, Turin, Italy.

**Stefano Olivares** received the Ph.D. degree in Physics from the University of Milan, Milano, Italy, and is currently a Researcher at the Department of Physics, University of Milan, Italy. He is a theoretician and his interests include quantum information, quantum estimation, quantum optics, quantum interferometry and quantum computation. His main contributions are in the fields of quantum estimation of states and operations, generation and application of entanglement, quantum information, communication and decoherence. Although his research activity is mainly theoretical, he is an active collaborator in many experimental groups. He is author of about 100 publications.

**Matteo G. A. Paris** received his Ph.D. in physics from University of Pavia, and is currently professor of quantum information and quantum optics at the Department of Physics of the University of Milan. His main contributions are in the fields of quantum estimation of states and operations, quantum tomography, generation, characterization and application of entanglement, quantum interferometry, nonclassical states and open quantum systems. In these fields he is author of about 250 publications in international journals. From 2013 he is editor-in-chief of *Quantum measurements and quantum metrology*.